T (908) 265-0096
vijay@telineage.com
www.telineage.com

Telineage
Bringing Trust Back To The Phone

Marlene H. Dortch
Secretary
Federal Communications Commision
445 12th Street, S.W.
Washington, D.C. 20554
Date 4/18/11

Re: Comments on WC Docket No. 11-39, Rules and Regulations implementing the Truth in Caller ID Act of 2009.

Dear Ms. Dortch,

We are appreciative of the efforts by the FCC in imposing rules and regulations to implement Truth to Caller ID. However, we believe it is equally important for the FCC to consider newer technologies that can be used in place of or in conjunction with Caller ID to both detect and prevent Caller ID spoofing. We would like to take this opportunity to introduce technology that was developed at the Georgia Tech Information Security Center (GTISC) to detect and prevent Caller ID spoofing and currently being commercialized by Telineage, a telecommunication security startup. Telineage's team consists of the lead researchers of this technology, who are wireline and wireless telecommunication security experts with patents and publications in the top security conferences.

Many currently deployed systems, including those from financial institutions, healthcare and the government, assume that the source information of a telephone call, such as Caller ID, can be trusted. For example, one criteria used by banks to allow activation of a credit card from a telephone is that the the Automatic Number Identification (ANI) or Caller ID of the calling phone is the same as that on file for the customer. Unfortunately, with the recent convergence of PSTN, cellular and voice over IP (VoIP) networks, Caller ID information is either not transferred between these networks or transferred without verification. This allows easy manipulation of this information and has resulted in several attacks including credit card fraud, identity theft, VoIP phishing, healthcare fraud and swatting that has cost individuals, enterprises and the government millions of dollars in losses.

The Truth to Caller ID Act of 2009 has made it illegal to "to cause any caller ID service to transmit misleading or inaccurate caller ID information". However, there are two issues with enforcing this regulation (11-39, para 29) -

1. It is hard to determine when Caller ID is spoofed and to detect the perpetrator of the attack, as they can easily use anonymization services like Tor to hide their activities.

2. It is applicable only to businesses headquartered in the US. Most Caller-ID spoofing uses VoIP and is carried out from any country, avoiding the legal ramifications of the act.

Regulation is most effective when there is a mechanism to detect wrongdoing and/or wrongdoers. However, Caller ID is completely broken and regulation coupled with alternative technologies has the best chance of success. The FCC should start considering feasible alternatives for the Caller ID service and provide these alternatives to Congress.

Telineage provides one such Caller ID alternative to secure transactions on the phone. It is based on our research, PinDr0p, at Georgia Tech that was published at a tier one security conference, ACM Computer and Communications Security (CCS) 2010. The research shows that regardless of the claimed source, the audio delivered to a call recipient exhibits measurable features of the source and the networks through which the call was delivered. For example, calls that traverse a VoIP network experience packet loss that results in perceivable effects in the final call audio. Such artifacts are noticeably absent in calls that have only traversed cellular or PSTN networks. There are many such artifacts specific to the calling phone and the network paths that allow us to develop profiles for call sources. Similar to fingerprints that identify humans, these profiles create a comprehensive phone fingerprint that uniquely identifies the phone.

As our technology only relies on analysis of audio at the receiving end, it requires no changes to be made to the telephony infrastructure. This is especially advantageous because of the complex and diverse nature of this infrastructure. We also note that though this does not provide the same guarantees as the use of end-to-end cryptography, it is also not encumbered with the difficulties of key distribution, management and the requirement that both endpoints are capable of such operations (for example, a traditional landline phone is incapable of cryptography). This technology can be used both to detect when Caller ID spoofing is occurring as well as prevent it.

We believe that in addition to imposing regulation on current Caller ID services, the FCC should also consider newer technologies that can be added to Caller ID to either prevent and/or detect Caller ID spoofing. We would welcome an opportunity to discuss our technology and provide further information on the comments provided above.

Sincerely yours,

Vijay A. Balasubramaniyan
CTO, Telineage